Basque CyberSecurity Centre

Actualización de seguridad de Microsoft-Diciembre 2022

BCSC-ACTUALIZACIONES-MICROSOFT-2022-DICIEMBRE

TLP: CLEAR

www.ciberseguridad.eus

EUSKO JAURLARITZA GOBIERNO VASCO

GRUPO spri TALDEA

TABLA DE CONTENIDO

Cláusula de exención de responsabilidad

El presente documento se proporciona con el objeto de divulgar las alertas que el BCSC considera necesarias en favor de la seguridad de las organizaciones y de la ciudadanía interesada. En ningún caso el BCSC puede ser considerado responsable de posibles daños que, de forma directa o indirecta, de manera fortuita o extraordinaria pueda ocasionar el uso de la información revelada, así como de las tecnologías a las que se haga referencia tanto de la web de BCSC como de información externa a la que se acceda mediante enlaces a páginas webs externas, a redes sociales, a productos de software o a cualquier otra información que pueda aparecer en la alerta o en la web de BCSC. En todo caso, los contenidos de la alerta y las contestaciones que pudieran darse a través de los diferentes correos electrónicos son opiniones y recomendaciones acorde a los términos aquí recogidos no pudiendo derivarse efecto jurídico vinculante derivado de la información comunicada.

Cláusula de prohibición de venta

Queda terminantemente prohibida la venta u obtención de cualquier beneficio económico, sin perjuicio de la posibilidad de copia, distribución, difusión o divulgación del presente documento.

Sobre el BCSC

El Centro Vasco de Ciberseguridad (Basque Cybersecurity Centre, BCSC) es la entidad designada por el Gobierno Vasco para elevar el nivel de madurez de la ciberseguridad en Euskadi.

Es una iniciativa transversal que se enmarca en la Agencia Vasca de Desarrollo Empresarial (SPRI), sociedad dependiente del Departamento de Desarrollo Económico, Sostenibilidad y Medio Ambiente del Gobierno Vasco. Así mismo, involucra a otros tres Departamentos del Gobierno Vasco: el de Seguridad, el de Gobernanza Pública y Autogobierno, y el de Educación, y a cuatro agentes de la Red Vasca de Ciencia, Tecnología e Innovación: Tecnalia, Vicomtech, Ikerlan y BCAM.

El BCSC es la entidad de referencia para el desarrollo de la ciberseguridad y de la confianza digital de ciudadanos, empresas e instituciones públicas en Euskadi, especialmente para los sectores estratégicos de la economía de la región.

La misión del BCSC es por tanto promover y desarrollar la ciberseguridad en la sociedad vasca, dinamizar la actividad empresarial de Euskadi y posibilitar la creación de un sector profesional que sea referente. En este contexto se impulsa la ejecución de proyectos de colaboración entre actores complementarios en los ámbitos de innovación tecnológica, investigación y transferencia tecnológica a la industria de fabricación avanzada y otros sectores.

Así mismo, ofrece diferentes servicios en su rol como Equipo de Repuesta a Incidentes (en adelante CERT, por sus siglas en inglés “Computer Emergency Response Team”) y trabaja en el ámbito de la Comunidad Autónoma del País Vasco para aumentar la capacidad de detección y alerta temprana de nuevas amenazas, la respuesta y análisis de incidentes de seguridad de la información, y el diseño de medidas preventivas para atender a las necesidades de la sociedad vasca. Con el fin de alcanzar estos objetivos forma parte de diferentes iniciativas orientadas a la gestión de incidentes de ciberseguridad:

FIRST Improving Security Together
TF-CSIRT Trusted Introducer
CSIRT.es

1. Resumen ejecutivo

Microsoft ha publicado las actualizaciones de seguridad del mes diciembre de 2022. Con estas actualizaciones se corrigen 51 vulnerabilidades, siendo 6 de ellas calificadas como críticas, 40 como importantes, 3 moderadas y 2 sin un valor asignado. Hay que destacar que dentro de ellas hay **2 zero-day**, **con una siendo explotada (CVE-2022-44710) y otra divulgada públicamente (CVE-2022-44698).**

A todas ellas se añaden 21 vulnerabilidades que afectan al navegador Edge basado en Chromium, que no disponen de un valor asignado, por parte Microsoft, en cuanto a su severidad e impacto.

Estas vulnerabilidades afectan a productos como Microsoft Office SharePoint, Microsoft Dynamics, Windows PowerShell, Windows Secure Socket Tunneling Protocol (SSTP) y Microsoft Edge (basado en Chromium), entre otros.

La clasificación de las vulnerabilidades según su descripción es la siguiente:

- 2 vulnerabilidad de bypass.
- 2 vulnerabilidades de denegación de servicio.
- 3 vulnerabilidades de divulgación de información.
- 23 vulnerabilidades de ejecución remota de código.
- 19 vulnerabilidades de elevación de privilegios.
- 2 vulnerabilidades de spoofing.

Por último, se destaca el aviso de seguridad ADV220005 añadido a las actualizaciones. Una guía de orientación sobre los controladores firmados por Microsoft que se utilizan de forma malintencionada.

2. Recursos afectados

Las actualizaciones de seguridad del mes de diciembre de 2022 están asociadas a vulnerabilidades que afectan a los siguientes productos:

- .NET Framework
- Azure
- Client Server Run-time Subsystem (CSRSS)
- Microsoft Bluetooth Driver
- Microsoft Dynamics
- Microsoft Edge (basado en Chromium)
- Microsoft Graphics Component
- Microsoft Office
- Microsoft Office OneNote
- Microsoft Office Outlook
- Microsoft Office SharePoint
- Microsoft Office Visio
- Microsoft Windows Codecs Library
- Role: Windows Hyper-V
- SysInternals
- Windows Certificates
- Windows Contacts
- Windows DirectX
- Windows Error Reporting
- Windows Fax Compose Form
- Windows HTTP Print Provider
- Windows Kernel
- Windows PowerShell
- Windows Print Spooler Components
- Windows Projected File System
- Windows Secure Socket Tunneling Protocol (SSTP)
- Windows SmartScreen
- Windows Subsystem for Linux

- Windows Terminal

3. Análisis técnico

A continuación, los detalles de las vulnerabilidades de más relevancia

corregidas en esta actualización son los siguientes:

Las 2 vulnerabilidades zero-day tratadas son:

CVE-2022-44710: vulnerabilidad de elevación de privilegios en el Kernel de gráficos DirectX, que **ha sido divulgada públicamente**. El fallo puede producir que un atacante que lo explotase con éxito pudiese obtener privilegios SYSTEM, lo que podría provocar un escape de entorno de ejecución contenido.

La métrica de evaluación de la vulnerabilidad se compone de:

CVSS Base: 7.8

CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H

- **Vector de ataque**: Local
- **Complejidad del ataque**: Alta
- **Privilegios requeridos:** Bajos
- **Interacción con el usuario**: **Ninguna**
- **Alcance**: **Con cambios**
- **Confidencialidad: Alta**
- **Integridad: Alta**
- **Disponibilidad: Alta**

CVE-2022-44698: vulnerabilidad de omisión de la característica de seguridad SmartScreen de Windows que **está siendo explotada.** Un atacante puede crear un archivo malintencionado que evadiría las defensas de la marca de la Web (MOTW), lo que provocaría una pérdida limitada de integridad y disponibilidad de características de seguridad como Vista protegida en Microsoft Office, que dependen del etiquetado MOTW.

La métrica de evaluación de la vulnerabilidad se compone de:

CVSS Base: 5.4

CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:L

- **Vector de ataque**: **Red**
- **Complejidad del ataque**: **Baja**
- **Privilegios requeridos:** Bajos
- **Interacción con el usuario**: Requerida
- **Alcance**: Sin cambios
- **Confidencialidad:** Ninguna
- **Integridad:** Baja
- **Disponibilidad:** Baja

Las vulnerabilidades críticas corregidas son:

CVE-2022-44690: vulnerabilidad de ejecución remota de código de Microsoft SharePoint Server. Un atacante autenticado con permisos para administrar lista podría ejecutar código de forma remota en el servidor de SharePoint.

La métrica de evaluación de la vulnerabilidad se compone de:

CVSS Base: 8.8

CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

- **Vector de ataque**: **Red**
- **Complejidad del ataque**: **Baja**
- **Privilegios requeridos:** Bajos
- **Interacción con el usuario**: **Ninguna**
- **Alcance**: Sin cambios
- **Confidencialidad: Alta**
- **Integridad: Alta**
- **Disponibilidad: Alta**

CVE-2022-44693: vulnerabilidad de ejecución remota de código de Microsoft SharePoint Server. Un atacante autenticado con permisos para administrar lista podría ejecutar código de forma remota en el servidor de SharePoint.

La métrica de evaluación de la vulnerabilidad se compone de:

CVSS Base: 8.8

CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

- **Vector de ataque**: **Red**
- **Complejidad del ataque**: **Baja**
- **Privilegios requeridos:** Bajos
- **Interacción con el usuario**: **Ninguna**
- **Alcance**: Sin cambios
- **Confidencialidad: Alta**
- **Integridad: Alta**
- **Disponibilidad: Alta**

CVE-2022-41127: vulnerabilidad de ejecución remota de código de Microsoft Dynamics NAV y Microsoft Dynamics 365 Business Central (local). La explotación exitosa de esta vulnerabilidad requiere que un atacante prepare el entorno de destino para mejorar la confiabilidad de la explotación, de manera que el puerto abierto de Dynamics NAV podría usarse para conectarse con el protocolo WCF TCP. Como usuario autenticado, el atacante podría intentar activar un código malicioso en el contexto de la cuenta del servidor a través de una llamada de red.

La métrica de evaluación de la vulnerabilidad se compone de:

CVSS Base: 8.5

CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H

- **Vector de ataque**: **Red**
- **Complejidad del ataque**: Alta
- **Privilegios requeridos:** Bajos
- **Interacción con el usuario**: **Ninguna**
- **Alcance**: **Con cambios**
- **Confidencialidad: Alta**
- **Integridad: Alta**
- **Disponibilidad: Alta**

CVE-2022-41076: vulnerabilidad de ejecución remota de código de PowerShell. La explotación exitosa de esta vulnerabilidad requiere que un atacante realice acciones adicionales antes de la explotación para preparar el entorno de destino, de tal manera que, podría escapar de la configuración de sesión remota de PowerShell y ejecutar comandos no aprobados en el sistema de destino.

La métrica de evaluación de la vulnerabilidad se compone de:

CVSS Base: 8.5

CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H

- **Vector de ataque**: **Red**
- **Complejidad del ataque**: Alta
- **Privilegios requeridos:** Bajos
- **Interacción con el usuario**: **Ninguna**
- **Alcance**: **Con cambios**
- **Confidencialidad: Alta**
- **Integridad: Alta**
- **Disponibilidad: Alta**

CVE-2022-44676: vulnerabilidad de ejecución remota de código del protocolo de túnel de sockets seguros (SSTP) de Windows. Un atacante no autenticado podría enviar una solicitud de conexión especialmente diseñada a un servidor RAS, lo que podría provocar la ejecución remota de código (RCE) en la máquina del servidor RAS.

La métrica de evaluación de la vulnerabilidad se compone de:

CVSS Base: 8.1

CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H

- **Vector de ataque**: **Red**
- **Complejidad del ataque**: Alta
- **Privilegios requeridos: Ningunos**
- **Interacción con el usuario**: **Ninguna**
- **Alcance**: Sin cambios

- **Confidencialidad: Alta**
- **Integridad: Alta**
- **Disponibilidad: Alta**

CVE-2022-44670: vulnerabilidad de ejecución remota de código del protocolo de túnel de sockets seguros (SSTP) de Windows. Un atacante no autenticado podría enviar una solicitud de conexión especialmente diseñada a un servidor RAS, lo que podría provocar la ejecución remota de código (RCE) en la máquina del servidor RAS.

La métrica de evaluación de la vulnerabilidad se compone de:

CVSS Base: 8.1

CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H

- **Vector de ataque**: **Red**
- **Complejidad del ataque**: Alta
- **Privilegios requeridos: Ningunos**
- **Interacción con el usuario**: **Ninguna**
- **Alcance**: Sin cambios
- **Confidencialidad: Alta**
- **Integridad: Alta**
- **Disponibilidad: Alta**

A continuación, se detalla la lista con todas las vulnerabilidades identificadas:

CVE	Descripción	Severidad	Divulgado	Explotado	CVSS
CVE-2022-44690	Vulnerabilidad de ejecución remota de código en Microsoft SharePoint Server	**Crítica**	No	No	8.8
CVE-2022-44693	Vulnerabilidad de ejecución remota de código en Microsoft SharePoint Server	**Crítica**	No	No	8.8
CVE-2022-41127	Vulnerabilidad de ejecución remota de código en Microsoft Dynamics NAV y Microsoft Dynamics 365 Business Central (local)	**Crítica**	No	No	8.5
CVE-2022-41076	Vulnerabilidad de ejecución remota	**Crítica**	No	No	8.5

	de código en PowerShell				
CVE-2022-44676	Vulnerabilidad de ejecución remota de código en el Protocolo de túnel de sockets seguros (SSTP) en Windows	**Crítica**	No	No	8.1
CVE-2022-44670	Vulnerabilidad de ejecución remota de código en el Protocolo de túnel de sockets seguros (SSTP) en Windows	**Crítica**	No	No	8.1
CVE-2022-41089	.Vulnerabilidad de ejecución remota de código en .NET Framework	Importante	No	No	8.8
CVE-2022-44708	Vulnerabilidad de elevación de privilegios en Microsoft Edge (basado en Chromium)	Importante	No	No	8.3
CVE-2022-44666	Vulnerabilidad de ejecución remota de código en Contactos de Windows	Importante	No	No	7.8
CVE-2022-44667	Vulnerabilidad de ejecución remota de código en Windows Media	Importante	No	No	7.8
CVE-2022-44668	Vulnerabilidad de ejecución remota de código en Windows Media	Importante	No	No	7.8
CVE-2022-44675	Vulnerabilidad de elevación de privilegios en el controlador Bluetooth de Windows	Importante	No	No	7.8

CVE-2022-44678	Vulnerabilidad de elevación de privilegios en la cola de impresión de Windows	Importante	No	No	7.8
CVE-2022-44680	Vulnerabilidad de elevación de privilegios en componentes gráficos de Windows	Importante	No	No	7.8
CVE-2022-44681	Vulnerabilidad de elevación de privilegios en la cola de impresión de Windows	Importante	No	No	7.8
CVE-2022-44683	Vulnerabilidad de elevación de privilegios en el kernel de Windows	Importante	No	No	7.8
CVE-2022-44691	Vulnerabilidad de ejecución remota de código en Microsoft Office OneNote	Importante	No	No	7.8
CVE-2022-44692	Vulnerabilidad de ejecución remota de código en Microsoft Office Graphics	Importante	No	No	7.8
CVE-2022-44694	Vulnerabilidad de ejecución remota de código en Microsoft Office Visio	Importante	No	No	7.8
CVE-2022-44695	Vulnerabilidad de ejecución remota de código en Microsoft Office Visio	Importante	No	No	7.8
CVE-2022-44696	Vulnerabilidad de ejecución remota de código en Microsoft Office Visio	Importante	No	No	7.8

CVE-2022-44702	Vulnerabilidad de ejecución remota de código en Terminal Windows	Importante	No	No	7.8
CVE-2022-44704	Vulnerabilidad de elevación de privilegios en Sysmon en Microsoft Windows	Importante	No	No	7.8
CVE-2022-26804	Vulnerabilidad de ejecución remota de código en Microsoft Office Graphics	Importante	No	No	7.8
CVE-2022-26805	Vulnerabilidad de ejecución remota de código en Microsoft Office Graphics	Importante	No	No	7.8
CVE-2022-26806	Vulnerabilidad de ejecución remota de código en Microsoft Office Graphics	Importante	No	No	7.8
CVE-2022-41094	Vulnerabilidad de elevación de privilegios en Windows Hyper-V	Importante	No	No	7.8
CVE-2022-41077	Vulnerabilidad de elevación de privilegios en formularios de redacción de fax de Windows	Importante	No	No	7.8
CVE-2022-41121	Vulnerabilidad de elevación de privilegios en componentes gráficos de Windows	Importante	No	No	7.8
CVE-2022-44671	Vulnerabilidad de elevación de privilegios en componentes	Importante	No	No	7.8

	gráficos de Windows				
CVE-2022-44687	Vulnerabilidad de ejecución remota de código en la extensión de imagen sin procesar	Importante	No	No	7.8
CVE-2022-44689	Vulnerabilidad de elevación de privilegios en el kernel del subsistema de Windows para Linux (WSL2)	Importante	No	No	7.8
CVE-2022-44710	Vulnerabilidad de elevación de privilegios en el kernel de gráficos DirectX	Importante	Sí	No	7.8
CVE-2022-47211	Vulnerabilidad de ejecución remota de código en Microsoft Office Graphics	Importante	No	No	7.8
CVE-2022-47212	Vulnerabilidad de ejecución remota de código en Microsoft Office Graphics	Importante	No	No	7.8
CVE-2022-47213	Vulnerabilidad de ejecución remota de código en Microsoft Office Graphics	Importante	No	No	7.8
CVE-2022-44713	Vulnerabilidad de suplantación de identidad en Microsoft Outlook para Mac	Importante	No	No	7.5
CVE-2022-44673	Vulnerabilidad de elevación de privilegios del subsistema de tiempo de ejecución (CSRSS) de	Importante	No	No	7.0

	cliente servidor de Windows				
CVE-2022-44669	Vulnerabilidad de elevación de privilegios en Informe de errores de Windows	Importante	No	No	7.0
CVE-2022-44682	Vulnerabilidad de denegación de servicio en Windows Hyper-V	Importante	No	No	6.8
CVE-2022-41115	Vulnerabilidad de elevación de privilegios en la actualización de Microsoft Edge (basada en Chromium)	Importante	No	No	6.6
CVE-2022-44679	Vulnerabilidad de divulgación de información en componentes gráficos de Windows	Importante	No	No	6.5
CVE-2022-44707	Vulnerabilidad de denegación de servicio en el kernel de Windows	Importante	No	No	6.5
CVE-2022-24480	Vulnerabilidad de elevación de privilegios en Outlook para Android	Importante	No	No	6.3
CVE-2022-44674	Vulnerabilidad de divulgación de información del controlador Bluetooth de Windows	Importante	No	No	5.5
CVE-2022-41074	Vulnerabilidad de divulgación de información en componentes gráficos de Windows	Importante	No	No	5.5

CVE-2022-44699	Vulnerabilidad de bypass de la característica de seguridad del agente de Azure Network Watcher	Importante	No	No	5.5
CVE-2022-44697	Vulnerabilidad de elevación de privilegios en componentes gráficos de Windows	Moderada	No	No	7.8
CVE-2022-44698	Vulnerabilidad de bypass de la característica de seguridad SmartScreen de Windows	Moderada	No	Sí	5.4
CVE-2022-44688	Vulnerabilidad de suplantación de identidad en Microsoft Edge (basado en Chromium)	Moderada	No	No	4.3
ADV220005	Guía sobre los controladores firmados de Microsoft que se utilizan con fines malintencionados	Sin valor asignado	No	No	7.8
CVE-2022-44677	Vulnerabilidad de elevación de privilegios proyectada del sistema de archivos de Windows	Sin valor asignado	No	No	7.8
CVE-2022-4174	Chromium: Confusión de tipo en V8	Sin valor asignado			
CVE-2022-4175	Chromium: Uso libre en captura de cámara	Sin valor asignado			
CVE-2022-4177	Chromium: Uso libre en Extensiones	Sin valor asignado			

CVE-2022-4178	Chromium: Uso libre en Mojo	Sin valor asignado			
CVE-2022-4179	Chromium: Uso libre en Audio	Sin valor asignado			
CVE-2022-4180	Chromium: Uso libre en Mojo	Sin valor asignado			
CVE-2022-4181	Chromium: Uso libre en Forms	Sin valor asignado			
CVE-2022-4182	Chromium: Implementación inadecuada en marcos cercados	Sin valor asignado			
CVE-2022-4183	Chromium: Aplicación insuficiente de directivas en Popup Blocker	Sin valor asignado			
CVE-2022-4184	Chromium: Aplicación insuficiente de directivas en Autorrelleno	Sin valor asignado			
CVE-2022-4185	Chromium: Implementación inadecuada en la navegación	Sin valor asignado			
CVE-2022-4186	Chromium: Validación insuficiente de entradas que no son de confianza en Descargas	Sin valor asignado			
CVE-2022-4187	Chromium: Aplicación insuficiente de directivas en DevTools	Sin valor asignado			
CVE-2022-4188	Chromium: Validación insuficiente de entradas que no son de confianza en CORS	Sin valor asignado			
CVE-2022-4189	Chromium: Aplicación insuficiente de	Sin valor asignado			

	directivas en DevTools				
CVE-2022-4190	Chromium: Validación de datos insuficiente en el Directorio	Sin valor asignado			
CVE-2022-4191	Chromium: Uso libre en el inicio de sesión	Sin valor asignado			
CVE-2022-4192	Chromium: Uso libre en Live Caption	Sin valor asignado			
CVE-2022-4193	Chromium: Aplicación insuficiente de directivas en la API del sistema de archivos	Sin valor asignado			
CVE-2022-4194	Chromium: Uso libre en Accesibilidad	Sin valor asignado			
CVE-2022-4195	Chromium: Aplicación insuficiente de directivas en Navegación segura	Sin valor asignado			

4. Mitigación / Solución

Para la mitigación y la corrección de todas las vulnerabilidades, Microsoft publica las actualizaciones de seguridad pertinentes junto con sus release notes, las cuales están disponibles en Security Update Guide.

5. Referencias Adicionales

- December 2022 Security Updates
- Security Update Guide - Microsoft
- Zero Day initiative-The December 2022 Security Update Review


Basque
CyberSecurity
Centre


EUSKO JAURLARITZA
GOBIERNO VASCO


GRUPO
spri
TALDEA